Chapter 6

The WATA Family

In this chapter, we focus on a family of computer-assisted exam protocols called WATA, which stands for Written Authenticated Though Anonymous exams. A common characteristic of all WATA protocols is the traditional testing procedure, which is face-to-face. The difference among the WATA protocols is that each version provides a different level of computer assistance. Additionally, each protocol of the family has some slightly different functional requirement and threat model with respect to the others. One protocol considers local tasks, such as notification of marks, and no TTP. Some others consider remote tasks, such as remote registration, but assume TTP. Another achieves remote tasks without TTP. In some way, Remark! already makes remote registration and remote notification with minimal reliance on trusted parties. As Remark! belongs to the class of Internet-based exams, it mandates candidate and exam authority to use computers at testing to sign and encrypt the tests. Therefore, testing cannot take place by pen and paper. Moreover, Remark! assumes at least one honest mix server. As we shall see later, there exists a version of WATA that ensures the same authentication and privacy requirements of Remark! without the need to rely on mixnet or TTP.

The various versions of WATA progressively introduce more computer assistance in their design still keeping traditional testing. The design of WATA I, II, and III has a high reliance on trusted parties. The design of WATA IV sees a lightweight participation of a TTP, and also opens up for computer-based exams. Moreover, it ensures more security requirements despite a stronger threat model. WATA IV is further reconceived to completely remove the TTP by combining oblivious transfer and visual cryptography to allow candidate and examiner to jointly generate a pseudonym that anonymises the candidate’s test. This pseudonym is revealed only to the candidate at the beginning of the face-to-face testing. This latter protocol proves to be secure by a formal analysis in ProVerif, which demonstrates that the protocol meets all the stated security requirements.

This chapter provides descriptions of all the WATA protocols available in the literature. It allows us to appreciate the different trade-offs between functional and security requirements in each of the WATA version.
Notification Request Authentication

The WATA exam was originally conceived for university exams, and in some universities nowadays candidates can take the exam up to a fixed number of times. However, if the candidate withdraws, it is not counted towards the number of attempts. Other universities have a policy that does not allow the candidate to resit a failed exam the next session, unless the candidate withdraws from the exam before notification. Thus, WATA exams consider the additional requirement of Notification Request Authentication. It says that a mark should be associated with the candidate only if she requests to learn her mark.

To formalise this requirement in the applied π-calculus, we need to define two new events that extend the list proposed in Chapter 3.

- \(\text{requested}(id_c, id_{test})\) means that the candidate \(id_c\) accepts to learn the mark associated to the test \(id_{test}\). The event is inserted into the process of the candidate at the location where the request is sent to the notifier.

- \(\text{stored}(id_c, mark)\) means that the authority officially considers the candidate \(id_c\) associated with \(mark\). The event is inserted into the process of the authority at the location where it registers the mark to the candidate.

The requirement can be specified as follows:

**Definition 43 (Notification Request Authentication)** An exam protocol ensures Notification Request Authentication if for every exam process \(EP\)

\[
\text{stored}(id_c, mark) \leadsto \text{inj}\text{requested}(id_c, id_{test})
\]

on every execution trace.

We use the specification above to formally analyse the protocol described in Section 6.5.

Outline of the chapter. Section 6 discusses existing schemes for computer-assisted and computer-based exams. Section 6.2 describes WATA I & II protocols and their informal analyses. Section 6.3 details WATA III. Section 6.4 introduces WATA IV according to the four phases of an exam and points up the novel security aspects respect to the previous WATA schemes. Section 6.5 redesigns parts of WATA IV to remove the TTP. It also introduces the formalisation of dispute resolution, and provides the formal analysis of the protocol in ProVerif. Section 6.6 discusses future work and ends the chapter.

6.1 Computer-Assisted and Computer-Based Exams

Nowadays, most of the exams employed in public competitions are computer-assisted or even computer-based. ETS and Pearson Vue develop various Computer-assisted exams for skill and professional certifications [ETS15, Pea15]. The European Union adopts computer-based exams for the selection of EU personnel [Off13]. The specification of such exams is not publicly available,